Incident Response Plan

Ben Tillis

Jerome Abe

Leroy Fry

Roy Jones

Fred Brown

Name of School

Date

Manager IT Department

Pixelated Pony Corporation

08 February 2016

Chief Information Officer

Pixelated Pony Corporation

RE: ANALYSIS OF CURRENT INCIDENT RESPONSE PLAN

An Incident Response Plan is an outline of procedure implemented in case any form of cyber-attack faces the organization (Francis, 2016). The plan outlines steps followed to mitigate the damage while maintaining the integrity of the organization’s computer system. Due to the increase in levels of cyber-threat, the current Incident Response Plan (IRP) should be reviewed for weaknesses and opportunities of improvement in the aspect of response team members and procedures.

The current IRP of the Pixelated Pony Company (PPC) has an outside source listed amongst the emergency contacts; this outside source to be is not properly specified or identified. The source to be contacted is, thus, vague and ambiguous. The emergency contact source of the organization may also not be familiar with the organization’s practices or may lack diligence or vigilance to deal with the situation. The details of the person, enlisted as an outside source of emergency team, should be provided, although the use of an outside member is highly discouraged as it may disrupt the plan, order or even sabotage the entire procedure.

The rest of the emergency contacts should also be evaluated. The response team to a cyber threat should be conversant with Information and Communication technology. As a result, the emergency team members should be selected based on their knowledge in the field of cyber technology, not according to positions of power within the organization (UC Berkley, 2016). Therefore, the business partner and manager specified as members of the PPC response team should be evaluated as members of the team. The members of the team should be explicitly selected for accountability and responsibility. The role of each specific member of the team should also be identified. This will help in maintaining order during the crisis, as the participants know what is expected of them. The contact information of the members of the team should also be present in the Incident Response Plan of the PPC organization. This will enable quick spreading of information regarding the threat or emergency to the relevant members.

An efficient Incident Response Plan should allocate emergency meeting sites for the team dealing with or handling the emergency (ENISA, 2016). The present IRP only caters for the communication channel of email between the corresponding emergency handlers. A centralized conference room for the team is required for briefing and updates regarding an ongoing situation. General notifications can also be provided within the specified physical area. The room should also contain any necessary equipment such as personal computer terminals that have access to the organization’s network. The management should designate this room in the IRP to prevent any hindrances or inconveniences that may be presented by random room allocation, which may lead to more chaos during a situation.

The members of the response team should be equipped with detailed information regarding the threat faced by the PPC organization. This will enable preparedness incase the threat is repeated, or analysis of any weaknesses that may facilitate the threat. Therefore, the IT security staff in charge of contacting the members should provide as detailed information as possible. As such, information regarding the details of targeted system, IP address, and location should not be withheld. This information is crucial to the team’s plan formulation, hence, should be availed as soon as possible. The handling of the communication channel should also not be the responsibility of one person. Due to the importance of maintaining communication between the team during the crisis, a specific team in charge of communication channel should be identified.

The Incident Response Plan should help in saving time and resources whilst coping with the incident of cyber threat. Hence, the procedures set up should avoid any repetition to save time and resources. In the current IRP of the organization, the assessing of the incident regarding the nature and the accompanying classification has been done thrice. This can be avoided by combining the three stages of assessment into one simple form of assessment in order to produce consistent and conclusive conclusion regarding the threat’s nature by the team in charge. Therefore, the assessment by the responder, the team over email, and the creation of incident ticket should be combined into one procedure. After the evaluation in which the entire team should participate, the nature of threat and the accompanying incident ticket should be known. The assessment of viruses and worms independently also complicates the entire assessment. The worm is a type of malware, and hence should be assessed in a similar manner as the entire body of viruses (malware).

As stated earlier, one of the main objectives of the response plan is to save time that would otherwise be wasted panicking during the crisis. As a result, the plan should be constrained within a set amount of time for efficient and smooth flow of the required operation. The response time for each specified action should be set to guide the team through the period required to undertake the process. The time specification for the current response plan is absent. This may lead to lagging of various participants during an attack.

An IRP is specific to the organization for which it serves (Queensland Government, 2016). In this regard, all aspects of the plan should be customized to meet the specified organization’s needs and requirements. The provided plan is not entirely customized for the PPC organization, as seen in the seventh step, which claims that the application may vary according to the organization implementing it. This should be corrected to suit the PPC exclusively for maximum achievement of objectives and mitigation of threats.

Data repository is a crucial aspect for future analysis (Francis, 2016). Therefore, data backup should be an essential aspect of the plan. This ensures that data to replace the corrupted one during an attack is available.

Lastly, after fending off an attack and the subsequent documentation, the IT team should seek after reviewing the security measures involved in the cyber-attack on the PPC organization. This should be accompanied by upgrade of the security measures throughout the entire organization’s system. This will help prevent future attacks similar to past ones.

In conclusion, the current Incident Response Plan has weaknesses that require revisiting for maximum preparedness. This will help upgrade the security measures of the PPC organization in accordance with the FBI warning. The weaknesses involve procedures and protocols that do not fully exploit the opportunities available or fail to acknowledge the full level of the threat facing the organization. The implemented IRP should then be constantly tested and reviewed by experts to ensure that it is up for the task, should the need arise.

References

Francis, R. (2016). *9 Steps for a successful incident response plan*. Retrieved from http://www.csoonline.com/article/3099684/disater-recovery/9-steps-for-a-successful-incident-response-plan.html

UC Berkley. (2016). *Incident response planning guideline.* Retrieved from http://ww.security.berkeley.edu/incident-response-planning-guideline

Queensland Government. (2016). *Preparing an incident response plan.* Retrieved from http://www.business.dld.gov.au/running-business/protecting-business/risk-management/incident-response

ENISA. (2016). *Incident Response Plan*. Retrieved from http://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/bcm-resilience/bc-plan/incident-response-plan